NIST Special Publication 800-76-1

Draft

Biometric Data Specification for Personal Identity Verification

**National Institute of
Standards and Technology**
Technology Administration
U.S. Department of Commerce

Charles Wilson

Patrick Grother

Ramaswamy Chandramouli

INFORMATION SECURITY

Information Technology Laboratory

National Institute of Standards and Technology

Gaithersburg, MD, 20899-8940

September 14, 2006

NOTE FOR REVIEWERS

1. This document is the draft of SP 800-76-1. It differs from the February 1, 2006 original by incorporating the following modifications.
    a. The edits previously published in the errata document.
    b. Typographical fixes and aesthetic changes not previously published.
    c. Relocation of material on template product certification from Section 7 into Section 8.
    d. Introduction and deletion of material from Section 7 to improve conformance of NIST's Minex test to SP 800-76. This includes deletion of misinterpreted material on "API specs".
    e. Clarification in Section 7, paragraph 1, that Section 7 regulates tests not products.
    f. Text to caution operators to acquire all ten fingers in plain impressions and to require rotation of (slap-acquired) fingerprint images prior to PIV minutiae template generation.
    g. Text requiring 14 rolled prints (i.e., Option 2) and Type 4 has not been included. It assumes a publication of overriding guidance from OMB.
    h. A clarification, initiated by a recent PIV Frequently Asked Questions, that single finger certification is only required for fingerprint products that use the mandatory templates.

2. Please submit your SP 800-76-1 comments using the comment template form provided on the http://www.csrc.nist.gov/piv-project/fips201-support-docs.html website.

3. Comments should be submitted to PIV_comments@nist.gov. Please include "Comments on Public Draft SP 800-76-1 in the subject line.

4. The comment period closes at 5:00 EST (US and Canada) on October 5, 2006. Comments received after the comment period closes will be handled on as-time-is-available basis.

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in Federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

ACKNOWLEDGEMENTS

EXECUTIVE SUMMARY

The Homeland Security Presidential Directive HSPD-12 called for new standards to be adopted governing the interoperable use of identity credentials to allow physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) standard for Federal Employees and Contractors, Federal Information Processing Standard (FIPS 201), was developed to establish standards for identity credentials. This document, Special Publication 800-76 (SP 800-76), is a companion document to FIPS 201. It describes technical acquisition and formatting specifications for the biometric credentials of the PIV system, including the PIV Card[1] itself. It enumerates procedures and formats for fingerprints and facial images by restricting values and practices included generically in published biometric standards. The primary design objective behind these particular specifications is high performance universal interoperability. For the preparation of biometric data suitable for the Federal Bureau of Investigation (FBI) background check, SP 800-76 references FBI documentation, including the ANSI/NIST Fingerprint Standard and the Electronic Fingerprint Transmission Specification. This document does not preclude use of other biometric modalities in conjunction with the PIV card.

---

[1] A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, biometric data) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This recommendation is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This recommendation has been prepared for use by federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should this recommendation be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the Office of Management and Budget, or any other Federal official.

1.2 Purpose and scope

FIPS 201 [FIPS], Personal Identity Verification (PIV) for Federal Employees and Contractors, defines procedures for the PIV lifecycle activities including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS also defines the structure of an identity credential which includes biometric data. Requirements concerning cryptographic protection of the biometric data are also described in [FIPS] and in [800-78].

This document contains technical specifications for biometric data mandated in [FIPS]. These specifications reflect the design goals of interoperability and performance of the PIV Card. This specification addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The goals are addressed by citing biometric standards normatively and by enumerating requirements where the standards include options and branches. In such cases, a biometric profile can be used to elucidate required versus optional content. This document goes further by constraining implementers' interpretation of the standards. Such restrictions are designed to ease implementation, assure conformity, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.

Thus, this document specifies various pieces of biometric data, and the processes used during and after their acquisition. However, for both logical and physical access applications, and for applications using biometric data stored either on or off the PIV Card, this document neither requires nor precludes the use of:

1. the PIV Card fingerprint templates;
2. specific authentication paradigms such as match-on-card;
3. data from other biometric modalities (e.g., hand geometry, iris, etc.);
4. data formatted according to other standards;
5. data whose format is proprietary or otherwise undisclosed.

This document does however specify that all biometric data to be embedded in the Common Biometric Exchange Formats Framework (CBEFF) structure of section 6. This document provides an overview of the strategy that can be used for testing conformance to the standard. It is not meant to be a comprehensive set of

test requirements that can be used for certification or demonstration of compliance to the specifications in this document.

1.3   Audience, assumptions, and overview

This document is targeted at Federal agencies and implementers of PIV systems. Readers are assumed to have a working knowledge of biometric standards and applications. This document defines, in section 3, the fingerprint acquisition process, and the retention and minutia generation formats. In section 4 it puts requirements on fingerprint mediated verification implementations, and specifies, in section 5, a facial image acquisition and retention format. Section 6 defines the generic header for all PIV biometric data. Sections 7 and 8 cover, respectively, certification and conformance tests. Finally section 9 is the bibliography.

2.   Terms, acronyms, and notation

2.1   Terms

Term	Definition
Segmentation	For fingerprints, segmentation is the separation of an N finger image into N single finger images.

2.2   Acronyms

Acronym	Definition
ANSI	American National Standards Institute
CBEFF	Common Biometric Exchange Formats Framework
FIPS	Federal Information Processing Standard
EFTS / F	Electronic Fingerprint Transmission Specification (Appendix F)
INCITS	InterNational Committee for Information Technology Standards
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NFIQ	NIST Fingerprint Image Quality
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification
WSQ	Wavelet Scalar Quantization

3.   Fingerprint enrollment

3.1   Scope

The specifications in this section pertain to the production of the mandatory PIV biometric enrollment data. That is, this section provides specifications for acquisition, formatting, and storage of fingerprint images and templates. The following is an overview of the material covered in this section.

+   Section 3.2 gives specifications for the use of fingerprint scanners to capture fingerprint images for PIV Registration;

+   Section 3.3 gives the format for fingerprint templates stored on the PIV Card;

+   Section 3.4 gives specifications for fingerprint images retained by agencies;

+   Section 3.5 specifies the transformation of fingerprints into records suitable for transmission to the FBI for the background check.

Note that although FBI requirements drive the sensor specifications, the permanent electronic storage formats, specified in Sections 3.3 and 3.4, are INCITS (i.e. non-FBI) standard records and are therefore specified independently. Figure 1 depicts the procedure for fingerprint acquisition and storage.

Figure 1 : PIV fingerprint image flow
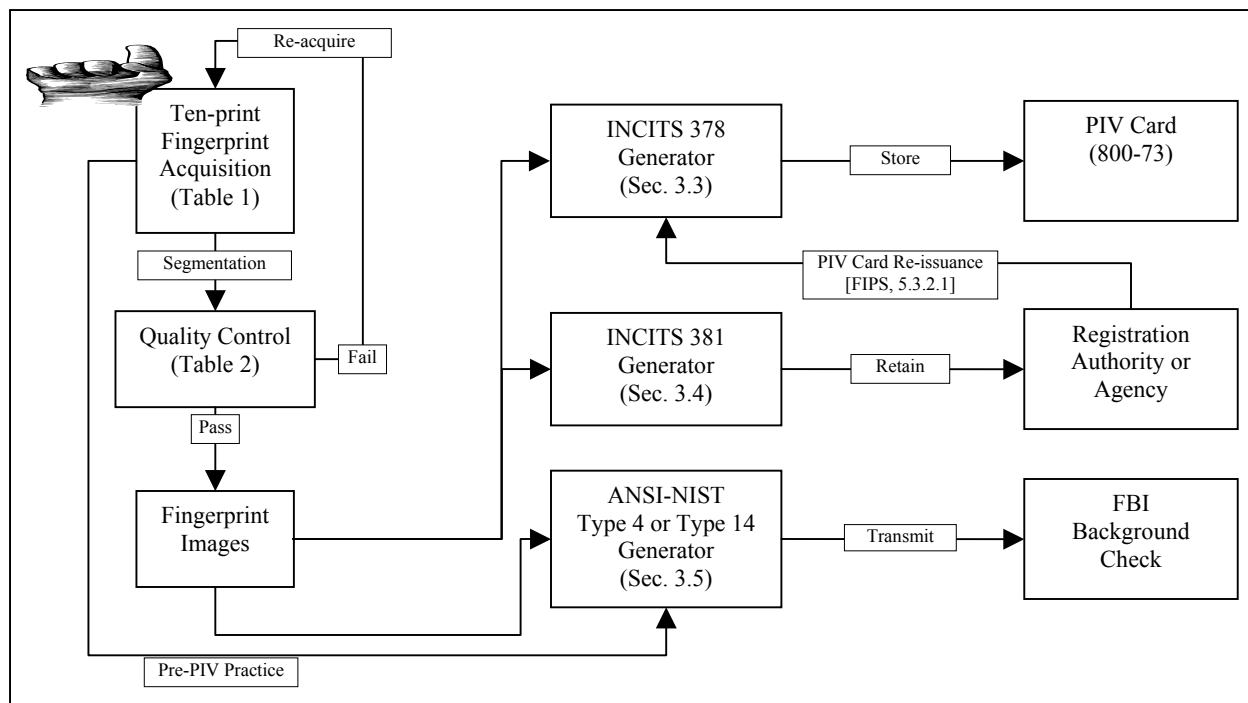
3.2   Fingerprint image acquisition

This section specifies the capture of a full set of fingerprint images for PIV registration. A subject's fingerprints shall be collected according to any of the three imaging modes enumerated in Table 1.

Table 1: Fingerprint acquisition protocols

Option 1 – Required presentations for plain live scan
Combined plain impression of the four fingers on the right hand (no thumb)
Combined plain impression of the four fingers on the left hand (no thumb)
Combined impression of the two thumbs
Option 2 – Required presentations for rolled live scan
10 separately rolled fingers
Combined plain impression of the four fingers on the right hand (no thumb)
Combined plain impression of the four fingers on the left hand (no thumb)
Left thumb plain impression   These captures may be simultaneous or sequential
Right thumb plain impression
Option 3 - Required presentations for rolled ink on card
10 separately rolled fingers
Combined plain impression of the four fingers on the right hand (no thumb)
Combined plain impression of the four fingers on the left hand (no thumb)
Left thumb plain impression   These captures may be simultaneous or sequential
Right thumb plain impression

INFORMATIVE NOTES:

1. There is no requirement that the order specified above is the order in which the images must be acquired.

2. The combined multi-finger plain-impression images are also referred to as slaps or flats. They are obtained by simultaneous placement of multiple fingers on the imaging surface without specific rolling movement.

3. Options 2 and 3 represent existing agency practice. Option 1 has recently become acceptable to the FBI.

For Options 1 and 2 the devices used for capture of the fingerprints shall have been certified by the FBI to conform to Appendix F of the FBI's Electronic Fingerprint Transmission Specification [EFTS, Appendix F]. For Option 3, a scan of the inked card shall be performed to effect conversion to electronic form. The scanner shall be certified by the FBI as being compliant with [EFTS, Appendix F]. The scanning is needed to produce fingerprints in the digital format described in Section 3.4 and thereby Section 3.5. The FBI specifications include width and height specifications for the imaging surface. The native scanning resolution of the device shall be 197 pixels per centimeter (500 pixels per inch) in both the horizontal and vertical directions. These specifications comply with the FBI submission requirements and with the Image Acquisition Setting Level 31 of the Finger Image-Based Data Interchange Format standard, INCITS 381 [FINGSTD].

The procedure for the collection of fingerprints, presented in Table 2, shall be followed. The procedure shall employ the NIST Fingerprint Image Quality [NFIQ] algorithm to initiate any needed reacquisition of the images. An attending official shall be present at the time of fingerprint capture. The official shall ensure that the applicant does not swap finger positions or hands, occlude fingers, or misalign or misplace the fingers. Particularly, because it is common during collection of multi-finger plain impressions for fingers 05 and 10 to not be long enough to reach the imaging platen, it is accepted practice for the hand be placed at an angle to the horizontal to ensure imaging of all four fingers. Although this is not needed with newer, large-platen, devices the official shall in all cases take care to image all fingers completely.   The procedure requires segmentation of the multi-finger plain impressions; this operation may be assisted by the attending official.

Table 2: Quality control procedure for acquisition of a full set of fingerprint images

Step	Action
1.	Attending official should inspect fingers and require absence of foreign material.
2.	Official should ensure imaging surface of the sensor, or the card, is clean.
3.	Acquire fingerprints according to Option 1, 2, or 3 in Table 1. For Option 3, scan the inked card using [EFTS, Appendix F] certified scanner.

4.	Segment the multi-finger plain impression images into single-finger images. Automated segmentation is recommended. Attending official should inspect the boundaries of the automatic segmentation and correct, via suitable user interface, any failures.
5.	Compute NFIQ value for thumbs and index fingers. If all have NFIQ values of 1, 2, or 3 (i.e., good quality) then go to step 8.
6.	Repeat steps 2-4 up to three more times.
7.	If after four acquisitions the index fingers and thumbs do not all have NFIQ values of 1, 2 or 3 then select that set, acquired in step 3 and segmented in step 4, for which the mean of the NFIQ values of the left index, right index, left thumb, and right thumb is minimum (i.e. of best quality). If all of the index finger and thumb quality values are unavailable (perhaps because of injury to one or more of those fingers) then use the last set from step 3 of those fingers that are available, without any application of NFIQ.
8.	Prepare and store the final records per Sections 3.3, 3.4, and 3.5

Ordinarily, all ten fingerprints shall be imaged in this process; however, if one or more fingers are not available (for instance, because of amputation) then as many fingers as are available shall be imaged. When fewer than ten fingers are collected, the FBI background transaction of Section 3.4 requires (in field AMP 2.084 of an accompanying Type 2 record) the labeling of those fingers that are amputated or otherwise not imaged; see [EFTS, Appendix C].

3.3   Fingerprint template specifications

This section specifies how the PIV mandatory biometric elements specified in [FIPS] are to be generated and stored. This specification applies to templates stored within the PIV Card, and to [MINUSTD] templates otherwise retained by agencies. The templates constitute the enrollment biometrics for PIV authentication and as such are supported by a high quality image acquisition specification, and a FBI-certified compression format. The specification of a standardized template in this section enables use of the PIV Card in a multi-vendor product environment.

3.3.1   Source images

Two [MINUSTD] fingerprint templates shall be stored on the PIV Card; these are hereafter referred to as PIV Card templates. These shall be prepared from images of the primary and secondary fingers (as specified in [FIPS]). These images shall be those obtained by segmenting the plain impressions of the full set of fingerprints captured during PIV Registration and stored in row 8 of Table 2.

Significant rotation of the multi-finger plain impressions (for example, that which can occur when four fingers are imaged using a narrow platen) shall be removed prior to, or as part of, the generation of the mandatory minutiae templates. The rotation angle shall be that which makes the inter-phalangeal creases approximately horizontal or, equivalently, the inter-finger spaces approximately vertical. This requirement supports interoperable fingerprint matching.

3.3.2   Minutia record

PIV Card templates shall be a conformant instance of the INCITS 378-2004 [MINUSTD] minutiae template standard. That is, the minutiae from both the primary and secondary fingers shall reside within a single INCITS 378 record. This means that there will be one instance of the "General Record Header" [MINUSTD, 6.4], and two instances of the "Finger View Record" [MINUSTD, 6.5]. This record shall be wrapped in a single instance of the CBEFF structure specified in Section 6 prior to storage on the PIV Card. The PIV Card templates shall not be encrypted.

Table 3 is a profile of the generic [MINUSTD] standard. Its specifications shall apply to all minutiae templates placed on PIV Cards. These constraints are included to promote highly accurate and interoperable personal identity verification. This document recommends that the minutiae records should be prepared after the images are captured and before they are compressed for storage (see Figure 1).

INCITS 378 is likely to be revised by the INCITS M1 committee. Such revisions are irrelevant to PIV; however implementations should respect the version number on Line 14 of Table 3.

When a PIV Card is issued, one or more authentication attempts shall be executed per [FIPS, 5.3.1]. This shall entail capture of new live fingerprints of both the primary and secondary fingers, and matching of those with the PIV Card templates. This binds the cardholder to the individual whose background was checked. This authentication may use a multi-finger fingerprint imaging device to capture single-finger images for authentication.

Table 3: INCITS 378 profile for PIV Card templates

|			Section title and/or field name (Numbers in parentheses are [MINUSTD] clause numbers)	INCITS 378-2004		PIV Conformance	Informative Remarks
				Field or content	Value Reqd	Values Allowed	
1.			Principle (5.1)	NC		A	Defines fingerprint minutiae
2.			Minutia Type (5.2)			See Note 6	[MINUSTD, 5.2] defines minutiae type but contains no normative content
3.			Minutia Location : Coordinate System (5.3.1)	NC		A	Definitions to be used when calculating minutia location.
4.			Minutia Location : Minutia Placement on a Ridge Ending (5.3.2)	NC		A	
5.			Minutia Location : Minutia Placement on a Ridge Bifurcation (5.3.3)	NC		A	
6.			Minutia Location : Minutia Placement on Other Minutia Types (5.3.4)	NC		See Note 6	
7.			Minutia Direction : Angle Conventions (5.4.1)	NC		A	Definitions to be used when calculating minutia angle.
8.			Minutia Direction : Angle of a Ridge Ending (5.4.2)	NC		A	
9.			Minutia Direction : Angle of a Ridge Bifurcation (5.4.3)	NC		A	
10.			Byte Ordering (6.2)	NC		A	Big Endian, unsigned integers
11.			Minutia Record Organization (6.3)	NC		A	
12.	General Record Header		CBEFF Record Header (6.4)	MF	MV	Patron format PIV	Multi-field CBEFF Header, Sec. 6.
13.			Format Identifier (6.4.1)	MF	MV	0x464D5200	i.e. ASCII "FMR\0"
14.			Version Number (6.4.2)	MF	MV	0x20323000	i.e. ASCII " 20\0" which is INCITS 378-2004. See Note 1
15.			Record Length (6.4.3)	MF	MV	26 ≤ L ≤ 800	This connotes a 2 byte field. See Note 2
16.			CBEFF Product Identifier Owner (6.4.4)	MF	MV	> 0	See Note 3
17.			CBEFF Product Identifier Type (6.4.4)	MF	MV	> 0	See Note 3
18.			Capture Equipment Compliance (6.4.5)	MF	MV	1000b	Sensor complies with EFTS, Appendix F per PIV Registration requirement
19.			Capture Equipment ID (6.4.6)	MF	MV	> 0	See Note 4
20.			Size of Scanned Image in x direction (6.4.7)	MF	MV	MIT	See Note 11
21.			Size of Scanned Image in y direction (6.4.8)	MF	MV	MIT	
22.			X (horizontal) resolution (6.4.9)	MF	MV	197	Parent images conform to section 3.3.1
23.			Y (vertical) resolution (6.4.10)	MF	MV	197	
24.			Number of Finger Views (6.4.11)	MF	MV	2	Once each for primary and secondary
25.			Reserved Byte (6.4.12)	MF	MV	0	
26.	K instances of the finger view record	View header	Finger View Header (6.5.1)	NC		A	
27.			Finger Position (6.5.1.1)	MF	MV	MIT	
28.			View Number (6.5.1.2)	MF	MV	0	See Note 10
29.			Impression Type (6.5.1.3)	MF	MV	0 or 2	Plain live or non-live scan images.
30.			Finger Quality (6.5.1.4)	MF	MV	20,40,60,80,100	See Note 5
31.			Number of Minutiae (6.5.1.5)	MF	MV	0 ≤ M ≤ 128	M minutiae data records follow
32.		instances of minutiae	Minutiae Type (6.5.2.1)	MF	MV	01b, 10b, or 00b	See Note 6
33.			Minutiae Position (6.5.2.2)	MF	MV	MIT	See Note 7
34.			Minutiae Angle (6.5.2.3)	MF	MV	MIT	See Note 8

			Section title and/or field name (Numbers in parentheses are [MINUSTD] clause numbers)	INCITS 378-2004		PIV Conformance	Informative Remarks
				Field or content	Value Reqd	Values Allowed	
35.			Minutiae Quality (6.5.2.4)	MF	MV	MIT	
36.			Extended Data Block Length (6.6.1.1)	MF	MV	0	See Note 9
END OF TABLE							

Acronym		Meaning
MF	mandatory field	[MINUSTD] requires a field shall be present in the FMR
MV	mandatory value	[MINUSTD] requires a meaningful value for a field
NC	normative content	[MINUSTD] gives normative practice for PIV. Such sections do not define a field in the FMR.
A	as required	For PIV, value or practice is as normatively specified in [MINUSTD].
MIT	mandatory at time of instantiation	For PIV, mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in [MINUSTD]

NORMATIVE NOTES:

1. The second paragraph of [MINUSTD, 6.4.2] refers both to an ASCII space and "three ASCII numerals" mentioned in the first paragraph. The practice of using an ASCII space character as the first character of the version number shall be followed: " 20\0" i.e. 0x20323000.

2. The length of the entire record shall fit within the container size limits specified in [800-73]. These limits apply to the entire CBEFF wrapped and signed entity, not just the [FINGSTD] record.

3. Both of the two fields ("Owner" and "Type") of the CBEFF Product Identifier of [MINUSTD, Section 6.4.4] shall be non-zero. The two most significant bytes shall identify the vendor, and the two least significant bytes shall identify the version number of that supplier's minutiae detection algorithm.

4. The Capture Equipment ID shall be reported. Its use may improve interoperability.

5. The quality value shall be that computed for the parent image using [NFIQ] and reported here as $Q = 20*(6 - NFIQ)$.

6. [MINUSTD] requires that each stored minutia have a type associated with it. For PIV, the mandatory card templates shall contain minutiae of type ridge ending or ridge bifurcation. These types are defined in [MINUSTD, 5.3.{2,3}]. Other types of minutiae, such as trifurcations and crossovers, shall not be included in PIV Card templates. However, for those minutiae where it is not possible to reliably distinguish between a ridge ending and a bifurcation, the category of "other" shall be assigned and encoded using bit values 00b. The angle and location for a minutia of type "other" should be the angle and location that would have applied to the corresponding ridge ending or bifurcation depending on which one the encoding algorithm determines to be the most likely for that particular minutiae. This is a common characteristic of "inked" impressions that exhibit ridge endings being converted to bifurcations and vice-versa due to over- or under-inking in the image.

7. All coordinates and angles for minutiae shall be recorded with respect to the original finger image. They shall not be recorded with respect to any image processing sub-image(s) created during the template creation process.

8. Determination of the minutia direction can be extracted from each skeleton bifurcation. The three legs of every skeleton bifurcation must be examined and the endpoint of each leg determined. Figures 2A through 2C illustrate the three methods used for determining the end of a leg. The ending is established according to the event that occurs first:

    o   The 32nd pixel – see Figures 2A and 2B – or

    o   The end of skeleton leg if greater than 10 pixels (legs shorter are not used) – see Figure 2B – or

    o   A 2nd bifurcation is encountered before the 32nd pixel – see Figure 2C.

    The angle of the minutiae is determined by constructing three virtual rays originating at the bifurcation point and extending to the end of each leg. The smallest of the three angles formed by the rays is bisected to indicate the minutiae direction.

Figure 2 : Minutiae angle determination
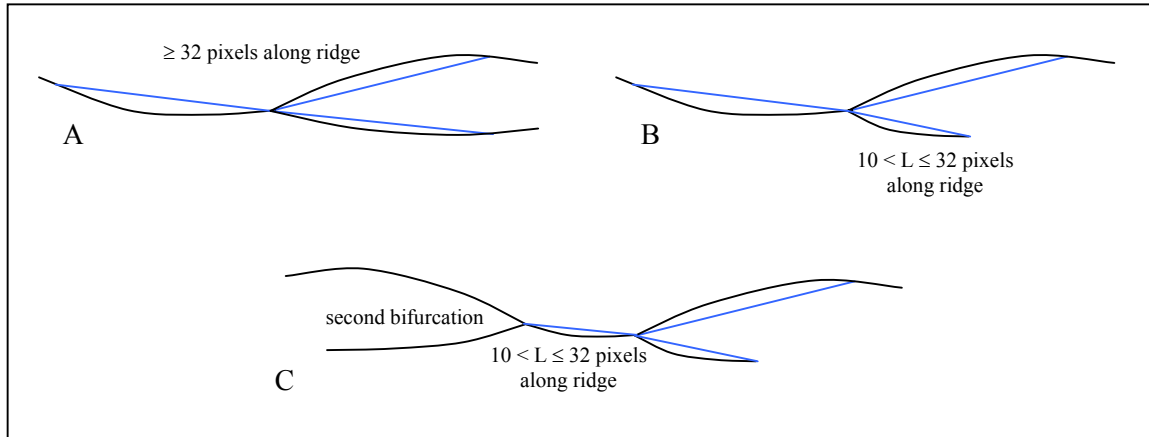
9. The mandatory value of zero codifies the specification that PIV card templates shall not include extended data.

10. Per [MINUSTD, 6.5.1.2] this view number field shall have value 0 for the primary finger and 0 for the secondary finger.   The combination of view number and finger position uniquely identifies each template.

11. [MINUSTD] does not specify how to report the image sizes in the header when two or more views are included in the record and these were derived from images of different sizes.   For PIV, the width on Line 20 shall be the larger of the widths of the two input images. Similarly the height on Line 21 shall be the larger of the heights of the two input images.

3.4   Fingerprint image format for images retained by agencies

This section specifies a common data format record for the retention of the fingerprint images collected in Section 3.2. Fingerprint images enrolled or otherwise retained by agencies shall be formatted according to the INCITS 381-2004 finger image based interchange format standard [FINGSTD]. This set shall include ten single-finger images. These shall be obtained by segmentation of the plain multi-finger images gathered in accordance with Options 1, 2 or 3 of Table 1, and the single plain thumb impressions from presentations 4 & 5 of Options 2 and 3. These images shall be placed into a single [FINGSTD] record. The record may also include the associated multi-finger plain impressions and the rolled images. This document ([800-76]) does not specify uses for any single-finger rolled images gathered according to Options 2 or 3 of Table 1. The record shall be wrapped in the CBEFF structure described in Section 6.

Table 4 gives a clause-by-clause profile of [FINGSTD]. The primary purpose of the Table is to give PIV specifications for those fields of [FINGSTD] that have optional content. Rows 2-11 give normative content. Row 11 requires the CBEFF structure of Section 6. However, its FASC-N value (Table 8, Line 13) may be replaced by a field of all zeroes in this one exceptional case: Storage of PIV registration images before a FASC-N has been assigned. Such instances (including the digital signature) shall be regenerated once the FASC-N is known. Rows 12-27 give PIV specifications for the fields of the General Record Header of [FINGSTD, Table 2]. These are common to all images in the record. Similarly, Rows 28-36 provide specifications for the Finger Image Header Record in Table 4 of [FINGSTD]. The penultimate column provides PIV specific practice and parameter defaults of the standard.

INCITS 381 is likely to be revised by the INCITS M1 committee. Such revisions are irrelevant to PIV; however implementations should respect the version number on Line 14 of Table 4.

Table 4: INCITS 381 profile for agency retention of fingerprint Images

			Section title and/or field name (Numbers in parentheses are [FINGSTD] clause numbers)	INCITS 381-2004		PIV Conformance	Informative Remarks
				Field or content	Value required	Values allowed	
1.			Byte and bit ordering (5.1)	NC		A	Big Endian MSB then LSB
2.			Scan sequence (5.2)	NC		A	
3.			Image acquisition reqs. (6)	NC		Level 31	Table 1
4.			Pixel Aspect Ratio (6.1)	NC		A	1:1
5.			Pixel Depth (6.2)	NC		A	Level 31 → 8
6.			Grayscale data (6.3)	NC		A	Level 31 → 1 byte per pixel
7.			Dynamic Range (6.4)	NC		A	Level 31 → 200 gray levels
8.			Scan resolution (6.5)	NC		A	Level 31 → 500 ppi
9.			Image resolution (6.6)	NC		197	Pixels per centimeter - no interpolation
10.			Fingerprint image location (6.7)	NC		A	Slap placement info, centering
11.			CBEFF Header (7)	MF	MV	Patron Format PIV	Multi-field CBEFF Header, Sec. 6
12.			General Record Header (7.1)	NC		A	
13.			Format Identifier (7.1.1)	MF	MV	0x46495200	i.e. ASCII "FIR\0"
14.			Version Number (7.1.2)	MF	MV	0x30313000	i.e. ASCII "010\0"
15.			Record Length (7.1.3)	MF	MV	MIT	Size excluding CBEFF structure
16.			CBEFF Product Identifier Owner (7.1.4)	MF	MV	> 0	CBEFF PID.
17.			CBEFF Product Identifier Type (7.1.4)	MF	MV	> 0	
18.			Capture Device ID (7.1.5)	MF	MV	MIT	Vendor specified. See Note 1
19.			Image Acquisition Level (7.1.6)	MF	MV	31	Settings Level 31
20.			Number of Images (7.1.7)	MF	MV	MIT	Denote by K, see lines 28-37. See Notes 2, 3 and 4
21.			Scale units (7.1.8)	MF	MV	0x02	Centimeters
22.			Scan resolution (horz) (7.1.9)	MF	MV	197	Pixels per centimeter
23.			Scan resolution (vert) (7.1.10)	MF	MV	197	
24.			Image resolution (horz) (7.1.11)	MF	MV	197	
25.			Image resolution (vert) (7.1.12)	MF	MV	197	
26.			Pixel Depth (7.1.13)	MF	MV	8	Grayscale with 256 levels
27.			Image compression algorithm (7.1.14)	MF	MV	0 or 2	Uncompressed or WSQ. See Notes 5 and 6.
28.			Reserved (7.1.15)	MF	MV	0	Two bytes, see Note 12
29.			Finger data block length (7.2.1)	MF	MV	MIT	
30.			Finger position (7.2.2)	MF	MV	MIT	
31.			Count of views (7.2.3)	MF	MV	≥ 1	M views of this finger, see Note 7
32.			View number (7.2.4)	MF	MV	MIT	
33.			Finger image quality (7.2.5)	MF	MV	20,40,60,80,100	Transformed NFIQ. See Notes 8 and 9
34.			Impression type (7.2.6)	MF	MV	0 or 2	See ANSI NIST ITL 1-2000
35.			Horizontal line length (7.2.7)	MF	MV	MIT	See Note 10
36.			Vertical line length (7.2.8)	MF	MV	MIT	
37.			Reserved (no clause)	MF	MV	0	See Note 11
38.			Finger image data (7.2.9)	MF	MV	MIT	Uncompressed or compressed WSQ Data

Rows 13–28 span column group "Finger image record format". Rows 29–38 span "K fingerprints, or multi-finger prints", and rows 32–38 span "M finger views".

END OF TABLE

Acronym		Meaning
MF	mandatory field	[FINGSTD] mandates a field shall be present in the record
MV	mandatory value	[FINGSTD] mandates a meaningful value for this field
NC	normative content	[FINGSTD] gives normative practice for PIV. Such sections do not define a field in the FIR.
A	as required by standard	For PIV, value or practice is as specified in [FINGSTD]
MIT	mandatory at time of instantiation	For PIV, mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in [FINGSTD]

NORMATIVE NOTES:

1. The Capture Device ID should indicate the hardware model. The CBEFF PID [FINGSTD, 7.1.4] should indicate the firmware or software version.

2. If certain fingers cannot be imaged, the value of this field shall be decremented accordingly.

3. The left and right four-finger images, and two-thumb, images may also be included. The value of this field shall be incremented accordingly.

4. For PIV enrollment sets, the number of images will ordinarily be thirteen (that is, the ten segmented images from the multi-finger plain impressions, and the three plain impressions themselves) or fourteen (if the plain thumb impressions were imaged separately).

5. Images shall either be uncompressed or compressed using an implementation of the Wavelet Scalar Quantization (WSQ) algorithm that has been certified by the FBI. The FBI's current requirement for a 15:1 nominal compression ratio shall apply.

6. Compression should only be applied after the records required by sections 3.3 and 3.5 have been prepared and transformed NFIQ values have been assigned.

7. The term view refers to the number of images of that particular finger. This value would exceed one if imaging has been repeated. Inclusion of more than one image of a finger can afford some benefit in a matching process. This document recommends that any additionally available images (say, from a PIV Card re-issuance procedure) with quality value 1 to 3 should be included in the record. In all cases the images shall be stored in order of capture date, with newest first.

8. Quality values shall be present. These shall be calculated from the NIST Fingerprint Image Quality (NFIQ) method described in [NFIQ] using the formula $Q = 20*(6 - NFIQ)$. This scale reversal ensures that high quality values connote high predicted performance and consistency with the dictionary definition. The values are intended to be predictive of the relative performance of a minutia based fingerprint matching system. It is recommended that a user should be prompted to first attempt authentication using the finger with the highest quality, regardless of whether this is the primary or secondary finger.

9. The quality value shall be set to 254 (the [FINGSTD] code for undefined) if this record is not a single finger print (i.e., it is a multi-finger image, or a palm print) or if the NFIQ implementation fails.

10. There is not restriction on the image size. However non-background pixels of the target finger shall be retained (i.e. cropping of the image data is prohibited).

11. [FINGSTD, Table 4] refers to a single-byte field labeled "reserved", but there is no corresponding clause to formally define it. The M1 committee has undertaken to resolve this by inserting a new subclause to require inclusion of the "Reserved" field. This will appear in a revision of [FINGSTD]. In any case, PIV implementations must include the single byte field, setting the value to 0.

12. Line 27 indicates that the "Reserved" field shall have length 2 bytes. [FINGSTD, 7.1.15] indicates a length of 4 bytes which disagrees with the value in [FINGSTD, Table 2]. The INCITS M1 committee has indicated 2 bytes is the correct value. PIV implementations shall include the 2 byte field, setting the value to 0.

3.5   Fingerprint image specifications for background checks

PIV fingerprint images transmitted to the FBI as part of the background checking process shall be formatted according to the ANSI/NIST-ITL 1-2000 standard [FFSMT] and the CJIS-RS-0010 [EFTS] specification. Such records shall be prepared from, and contain, only those images collected as per specifications in Section 3.1.

Table 5 enumerates the appropriate transaction formats for the three acquisition options of Section 3.2. The FBI documentation [EFTS] should be consulted for definitive requirements.

Table 5: Record types for background checks

Option	Transaction Data Format in [FFSMT]	Reference
1	Three Type 14 records.	[EFTS, Appendix N]. See Note 2
2 or 3	Fourteen Type 4 records	Section 3.1.1.4 "Federal Applicant User Fee" of [EFTS]

NORMATIVE NOTES:

1. All types of transactions with the FBI require both a Type 1 and Type 2 record to accompany the data; see [FFSMT, Table 2]. The Type 2 supports labeling of missing fingers.

2. The forthcoming ANSI/NIST-ITL revision (due in late 2006) will not alter the Appendix N specification. In any case Appendix N shall be the definitive reference.

4.   Sensor specifications for fingerprint verification

4.1   Scope

This section gives specifications for all fingerprint sensors used for capture of live authentication fingerprints (i.e. for the verification of PIV cardholders). This specification applies to any sensor involved in use of the mandatory PIV Card templates of section 3.3. These specifications are unrelated to those of section 3 which govern enrollment.

4.2   PIV authentication fingerprint acquisition specifications

Fingerprint sensors used for PIV authentication shall conform to the FBI's Image Quality Specifications For Single Finger Capture Devices [SINGFING]. Devices shall be capable of imaging an area of at least 12.8 millimeters horizontally x 16.5 millimeters vertically at a native resolution of at least 197 pixels per centimeter in each direction.

5.   Facial image specifications

5.1   Scope

[FIPS, Section 4.4.1] requires collection of a facial image from PIV applicants, and indicates that it may be used for generation of the printed image [FIPS, Section 4.1.4.1] and for augmentation of human authentication of the card holder. The face specification in this document supports those activities, and establishes a storage format for retention of facial images. As with other biometric elements, agencies may elect to store face data on the PIV card and use it for automated verification. Although this section places no normative requirements on such agency-optional activities, it does specify an image suited for automated biometric enrollment and face recognition.

5.2   Acquisition and format

This section provides specifications for the retention of facial images. Facial images collected during PIV Registration shall be formatted such that they conform to INCITS 385-2004 [FACESTD]. In addition to establishing a format, [FACESTD] specifies how a face image should be acquired. This is done to improve image quality and, ultimately, performance. The images shall be embedded within the CBEFF structure defined in Section 6. Because [FACESTD] is generic across applications it includes sections that have either-or requirements. Table 6 is an application profile of [FACESTD] tailored for PIV. It gives concrete specifications for much of the generic content. Column 3 references the sections of [FACESTD] and columns 4 and 5 give [FACESTD] requirements. For PIV, column 6 of Table 6 gives normative practice or value specifications. The table is not conformant with the Implementation Conformance Statement [ICS] standard. Particularly it extends the function of ICS but because it has the needed rows it may be useful in construction of a traditional ICS. Nevertheless the addition of a "values supported column" as specified in Section 9.1 of [ICS] should be used by implementers for checking conformance to the specifications.

INCITS 385 is likely to be revised by the INCITS M1 committee. Such revisions are irrelevant to PIV; however implementations should respect the version number on Line 14 of Table 6.

Table 6: INCITS 385 profile for PIV facial images

		Section title and/or field name (Numbers in parentheses are [FACESTD] clause numbers)	INCITS 385-2004		PIV Conformance	Informative Remarks
			Field or content	Value Reqd	Values Allowed	
1.		Byte Ordering (5.2.1)	NC		A	Big Endian
2.		Numeric Values (5.2.2)	NC		A	Unsigned Integers
3.	CBEFF	CBEFF Header (5.3)	MF	MV	Patron format PIV	Multi-field CBEFF Header. Sec. 6.
4.	Facial Header	Format Identifier (5.4.1)	MF	MV	0x46414300	i.e. ASCII "FAC\0"
5.		Version Number (5.4.2)	MF	MV	0x30313000	i.e. ASCII "010\0"
6.		Record Length (5.4.3)	MF	MV	MIT	See Note 1
7.		Number of Facial Images (5.4.4)	MF	MV	≥ 1	One or more images (K ≥ 1). See Notes 2 and 3, and also line 20.
8.	Facial Info. Single instance of subject-specific info.	Facial image Block Length (5.5.1)	MF	MV	MIT	
9.		Number of Feature Points (5.5.2)	MF	MV	≥ 0	Positive, if features computed
10.		Gender (5.5.3)	MF	OV	OIT	These fields populated with meaningful values at agency discretion, otherwise 0 for unspecified.
11.		Eye color (5.5.4)	MF	OV	OIT	
12.		Hair color (5.5.5)	MF	OV	OIT	
13.		Feature Mask (5.5.6)	MF	OV	OIT	
14.		Expression (5.5.7)	MF	OV	1	Neutral
15.		Pose Angles (5.5.8)	MF	OV	0	Unspecified = Frontal
16.		Pose Angle Uncertainty (5.5.9)	MF	OV	0	Attended operation so should be frontal.
17.	Features	MPEG4 Features (5.6.1)	NC		OIT	

		Section title and/or field name (Numbers in parentheses are [FACESTD] clause numbers)	INCITS 385-2004 Field or content	Value Reqd	PIV Conformance Values Allowed	Informative Remarks
18.	Image Info. Each instance has image-specific info.	Center of Facial Features (5.6.2)	NC		OIT	
19.		The Facial Feature Block Encoding (5.6.3)	OF	OV	OIT	
20.		Facial Image Type (5.7.1)	MF	MV	1	See Note 4.
21.		Image Data Type (5.7.2)	MF	MV	0 or 1	See Note 5. Compression algorithm.
22.		Width (5.7.3)	MF	MV	MIT	See Note 7.
23.		Height (5.7.4)	MF	MV	MIT	
24.		Image Color Space (5.7.5)	MF	MV	1	sRGB. See Note 8.
25.		Source Type (5.7.6)	MF	MV	2 or 6	Digital still or digital video
26.		Device Type (vendor supplied device ID) (5.7.7)	MF	MV	MIT	
27.		Quality (5.7.8)	MF	MV	A	[FACESTD] requires 0 (unspecified)
28.	Image Data	Data Structure (5.8.1)	MF	MV	MIT	Compressed Data
29.	Basic (section 6) — Inheritance	Inheritance (6.1)	NC		A	
30.		Image Data Encoding (6.2)	NC		A	See Note 5
31.		Image Data Compression (6.3)	NC		A	See Notes 5+6
32.	Format	Facial Header (6.4.1)	NC		A	Include 4 fields
33.		Facial Information (6.4.2)	NC		A	Include 9 fields
34.		Image Information (6.4.3)	NC		A	Include 8 fields
35.	Frontal (section 7) — Scene	Inheritance (7.1)	NC		A	Inherits Basic
36.		Purpose (7.2.1)	NC		A	frontal Annex A
37.		Pose (7.2.2)	NC		Frontal	+/- 5 degrees
38.		Expression (7.2.3)	NC		Neutral	
39.		Assistance in positioning face (7.2.4)	NC		A	Only the subject appears
40.		Shoulders (7.2.5)	NC		A	Body + Face toward camera
41.		Backgrounds (7.2.6)	NC		Annex A.4.3	Uniform
42.		Subject and scene lighting (7.2.7)	NC		A	Uniform
43.		Shadows over the face (7.2.8)	NC		A	None
44.		Eye socket shadows (7.2.9)	NC		A	None
45.		Hot spots (7.2.10)	NC		A	Should be absent. Diffuse light.
46.		Eye glasses (7.2.11)	NC		A	Subject's normal condition
47.		Eye patches (7.2.12)	NC		A	Medical only
48.	Photographic	Exposure (7.3.2)	NC		A	No saturation
49.		Focus and Depth of Field (7.3.3)	NC		A	In focus
50.		Unnatural Color (7.3.4)	NC		A	White balance
51.		Color or grayscale enhancement (7.3.5)	NC		A + no recompress	No post-processing
52.		Radial Distortion of the camera lens (7.3.6)	NC		A + Follow Annex A.8	
53.	Digital — Geometry	aspect ratio (7.4.2.1)			A	1:1 pixels
54.		origin (7.4.2.2)			A	top left is 0,0
55.	Color Profile	Density (7.4.3.1)	NC		A	7 bits dynamic range in gray
56.		Color Sat (7.4.3.2)	NC		A	7 bits dynamic once in grayscale
57.		Color space (7.4.3.3)	NC		24 bit RGB	Option a, reported in color space field above. See Note 8
58.		Video Interlacing (7.4.4)	NC		A	Interlaced sensors are not permitted.
59.	Full Frontal (section 8)	Inheritance (8.1)	NC		A	Inherits Frontal + Basic
60.		Scene (8.2)	NC		A	Inherits Frontal + Basic
61.	Photographic	Centered Image (8.3.2)	NC		A	Nose on vertical centerline
62.		Position of Eyes (8.3.3)	NC		A	Above horizontal centerline
63.		Width of Head (8.3.4)	NC		A	See Note 7
64.		Length of Head (8.3.5)	NC		A	See Note 7
65.	Digital	Resolution (8.4.1)	NC		CC ≥ 240	See Note 7

		Section title and/or field name (Numbers in parentheses are [FACESTD] clause numbers)	INCITS 385-2004		PIV Conformance	Informative Remarks
			Field or content	Value Reqd	Values Allowed	
66.	Format	Inheritance (8.5.1)	NC		A	
67.		Image Information (8.5.2)	NC		A	

END OF TABLE

Acronym		Meaning
FAC	Face Information Record	Facial header + facial info + repetition of (image info + image data)
MF	mandatory field	[FACESTD] requires a field shall be present in the FAC
OF	optional field	[FACESTD] allows a field to be present in record
MV	mandatory value	[FACESTD] requires a meaningful value for a field
OV	optional value	[FACESTD] allows a meaningful value or allows 0 to be used to connote "unspecified"
NC	normative content	[FACESTD] gives normative practice for PIV. Such sections do not define a field in the FAC.
A	as required	For PIV, value or practice is as specified in [FACESTD]
MIT	mandatory at time of instantiation	For PIV, mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in [FACESTD]
OIT	optional at time of instantiation	For PIV, optional header value that may be determined at the time the record is instantiated

NORMATIVE NOTES:

1. If facial imagery is stored on the PIV Card, the length of the entire record shall fit within the container size limits specified in [800-73]. These limits apply to the entire CBEFF wrapped and signed entity, not just the [FACESTD] record. Key lengths and signing algorithms are specified in [800-78]. The size of the digital signature scales with the key length; it does not scale with the size of the biometric record.

2. More than one image may be stored in the record. It may be appropriate to store several images if appearance changes over time (beard, no beard, beard) and images are gathered at re-issuance. The most recent image shall appear first and serve as the default provided to applications.

3. When facial imagery is stored on the PIV Card, only one image shall be stored.

4. PIV facial images shall conform to the Full Frontal Image Type defined in Section 8 of [FACESTD].

5. Facial image data shall be formatted in either of the compression formats enumerated in Section 6.2 of [FACESTD]. Both whole-image and single-region-of-interest (ROI) compression are permitted. This document ([800-76]) recommends that newly collected facial image should be compressed using ISO/IEC 15444 (i.e. JPEG 2000). This applies when images will be input to automated face recognition products for authentication, and when images are stored on PIV Cards. In this latter case, ROI compression should be used. The older ISO/IEC 10918 standard (i.e. JPEG) should be used only for legacy images.

6. Facial images shall be compressed using a compression ratio no higher than 15:1. However, when facial images are stored on PIV Cards JPEG 2000 should be used with ROI compression. The innermost region should be centered on the face and compressed at no more than 24:1.

7. Face recognition performance is a function of the spatial resolution of the image. [FACESTD] does not specify a minimum resolution for the Full Frontal Image Type. For PIV, faces shall be acquired such that a 20 centimeter target placed on, and normal to, a camera's optical axis at a range of 1.5 meters shall be imaged with at least 240 pixels across it. This ensures that the width of the head (i.e. dimension CC in Figure 8 of [FACESTD]) shall have sufficient resolution for the printed face element of the PIV Card. This specification and Section 8.3.4 of [FACESTD] implies that the image width shall exceed 420 pixels. This resolution specification shall be attained optically without digital interpolation. The distance from the camera to the subject should be greater than or equal to 1.5 meters (for distortion reasons discussed in [FACESTD, Annex A.8]). The size specification is a minimum: When images are to be used for automated face recognition higher resolution is likely to yield lower error rates.

8. Facial image data shall be converted to the sRGB color space if it is stored. As stated in Section 7.4.3.3 of [FACESTD] this requires application of the color profile associated with the camera in use.

6.   Common header for PIV biometric data

All PIV biometric data shall be embedded in a data structure conforming to Common Biometric Exchange Formats Framework [CBEFF]. This specifies that all biometric data shall be digitally signed and uniformly encapsulated. This covers: the PIV Card fingerprints mandated by [FIPS]; any other biometric data agencies elect to place on PIV Cards; any biometric records that agencies elect to retain (including purely proprietary, or derivative, elements); and any biometric data retained by, or for, agencies or Registration Authorities. The EFTS transaction data described in section 3.5 is exempt.

All such data shall be signed in the same manner as prescribed in [FIPS 201] and [800-73] for the mandatory biometric elements. The signature is present for integrity and shall be stored in the CBEFF signature block. The overall arrangement is depicted in Table 7.

Table 7: Simple CBEFF structure

CBEFF STRUCTURE		
CBEFF_HEADER	CBEFF_BIOMETRIC_RECORD	CBEFF_SIGNATURE_BLOCK
Section 6	Sections 3.3, 3.4 and 5.2	FIPS 201
INCITS 398 5.2.1	INCITS 398 5.2.2	INCITS 398 5.2.3

The CBEFF Header specified in Table 8 and its notes will be established by NIST as Patron Format "PIV". This format will be established as a formal Patron Format per the provisions of [CBEFF, 6.2]. It adds definitive data types and the FASC-N field mandated by [FIPS] to a subset of the fields given in Patron Format A [CBEFF, Annex A]. It exists independently of Patron Format A. All fields of the format are mandatory.

Table 8: Patron format PIV specification

	Patron Format PIV Field (Numbers in parentheses are [CBEFF] clause numbers)	Length Bytes	PIV Data Type	PIV Conformance Required Value
1.	Patron Header Version (5.2.1.4)	1	UINT	0x03
2.	SBH Security Options (5.2.1.1, 5.2.1.2)	1	Bitfield	See Note 2
3.	BDB Length	4	UINT	Length, in bytes, of the biometric data CBEFF_BIOMETRIC_RECORD
4.	SB Length	2	UINT	Length, in bytes, of the CBEFF_SIGNATURE_BLOCK
5.	BDB Format Owner (5.2.1.17)	2	UINT	See Note 4
6.	BDB Format Type (5.2.1.17)	2	UINT	See Note 5
7.	Biometric Creation Date (5.2.1.10)	8		See Note 6 for data type
8.	Validity Period (5.2.1.11)	16		See Note 7 for data type
9.	Biometric Type (5.2.1.5)	3	UINT	See Note 8
10.	Biometric Data Type (5.2.1.7)	1	Bitfield	See Note 9
11.	Biometric Data Quality (5.2.1.9)	1	SINT	See Note 10
12.	Creator (5.2.1.12)	18	Note 6	See Note 11 for data type
13.	FASC-N	25	Note 7	See Note 12 for data type
14.	Reserved for future use	4		0x00000000
END OF TABLE				

NORMATIVE NOTES:

1.   Unsigned integers are denoted by UINT. Signed integers are denoted by SINT. Multi-byte integers shall be in Big Endian byte order.

2. The security options field has two acceptable values. The value b00001101 indicates that the biometric data block is digitally signed but not encrypted; the value b00001111 indicates the biometric data block is digitally signed and encrypted. For the mandatory [MINUSTD] elements on the PIV Card the value shall be b00001101.

3. The fourth bit (mask 0x08) is set per prior versions of this document. The third bit (mask 0x04), which in each case is set, implements the [CBEFF, 5.2.1.2] requirement that digital signature is differentiated from message authentication code. The second bit (mask 0x02) indicates the use of encryption. The first bit (mask 0x01) indicates the use of a digital signature. Specifications for the computation of digital signatures are set forth in [800-78].

4. For fingerprint and facial records defined sections 3.3, 3.4 and 5 the Format Owner shall be 0x001B denoting M1, the INCITS Technical Committee on Biometrics. Otherwise see [CBEFF, 5.2.1.17].

5. For fingerprint image data defined above the Format Type shall be 0x0401. For the mandatory fingerprint minutiae template data this value shall be 0x0201. For face data this value shall be 0x0501. For other biometric records on the PIV Card or otherwise retained by agencies this field shall be assigned in accordance with the procedures of [CBEFF, 5.2.1.17].

6. This is the date that the biometric sample was acquired. For processed samples (e.g. templates) this data should be the date of acquisition of the parent sample. Creation Date shall be encoded in eight bytes using a binary representation of "YYYYMMDDhhmmssZ". Each pair of characters (for example, "DD") is coded in 8 bits as an unsigned integer. Thus 17:35:30 December 15, 2005 is represented as: 00010100 00000101 00001100 00001111 00010001 00100011 00011110 01011010 where the last byte is the binary representation of the ASCII character Z which is included to indicate that the time is represented in Coordinated Universal Time (UTC). The field "hh" shall code a 24 hour clock value.

7. The Validity Period contains two dates each of which shall be coded according to Normative Note 6.

8. For fingerprint images and any kind of fingerprint template the type shall be 0x000008, for facial images the type shall be 0x000002. The value for other biometric modalities shall be that given in [CBEFF, 5.2.1.5]. For modalities not listed there the value shall be 0x0.

9. [CBEFF, 5.2.1.7] establishes three categories for the degree to which biometric data has been processed. These are encoded in Table 9. For the mandatory [MINUSTD] PIV Card templates this value shall be b100xxxxx.

Table 9: CBEFF biometric data type encoding

Data Type	PIV Required Value	Examples of biometric data falling into category
Raw	b001xxxxx	[FACESTD] and [FINGSTD] images
Intermediate	b010xxxxx	
Processed	b100xxxxx	[MINUSTD] templates

10. For single [FINGSTD] fingerprint images or [MINUSTD] templates extracted from them, the quality value shall be $Q = 20*(6 - NFIQ)$ where NFIQ is computed using the method of [NFIQ]. When multiple views or samples of a biometric are contained in the record the largest (i.e. best) value should be reported. For all biometric data whether stored on a PIV Card or otherwise retained by agencies the quality value shall be a signed integer between -2 and 100 per the text of INCITS 358. A value of -2 shall denote that assignment was not supported by the implementation; a value of -1 shall indicate that an attempt to compute a quality value failed. Values from 0 to 100 shall indicate an increased expectation that the sample will ultimately lead to a successful match. The zero value required by [FACESTD] shall be coded in this CBEFF field as -2.

11. For PIV the Creator field has length 18 bytes of which the first $K \leq 17$ bytes shall be printable ASCII characters, and the first of the remaining 18-K shall be a null terminator (zero).

12. This field shall contain the 25 bytes of the FASC-N component of the CHUID identifier, per [800-73, 1.8.{3,4}].

7.   Performance testing and certification procedures

7.1   Scope

This section gives normative specifications for tests used to certify implementations that generate and/or match the mandatory biometric elements specified by [FIPS], i.e. the two fingerprint minutiae templates placed on the PIV Card. That is, this section regulates the test itself, not the products under test, and the data specifications here should not be confused with those given in Section 3 for fielded PIV implementations.

7.2   PIV authentication

The fingerprint templates conform to [MINUSTD] as profiled in section 3.3. The use cases given in [800-73, Appendix C] detail how the templates and the PIV Card are used for interoperable authentication. Authentication may involve one or both of the PIV Card templates. These will be compared with newly acquired (i.e. live) fingerprint images of either or both of the primary and secondary fingers. The inclusion of the finger position in the [MINUSTD] header allows a user to be prompted for their specific finger or fingers.

Authentication performance is quantified in terms of both the false reject rate (FRR) and the false accept rate (FAR). In PIV, the former would quantify the proportion of legitimate cardholders incorrectly denied access; the latter would be the proportion of impostors incorrectly allowed access. The error rates depend on a number of factors including: the environment, the number of attempts (i.e. finger placements on the sensor), the sensor itself, the quality of the PIV Card templates' parent images, the number of fingerprints invoked, and the familiarity of users with the process. The use of two fingers[2] in all authentication transactions offers substantially improved performance over single-finger authentication. The intent of the [FIPS] specification of an interoperable biometric is to support cross-vendor and cross-agency authentication of PIV Cards. This plural aspect introduces a source of variation in performance.

7.3   Test overview

This section specifies procedures for the certification of generators and matchers of [MINUSTD] templates.

Interoperability testing requires exchange of templates between products, which shall therefore be tested as a group. Accordingly, the test organization shall conduct a first round of testing to establish a primary group of interoperable template generators and matchers. Certification shall be determined quantitatively at the conclusion of the test. Thereafter certification requires interoperability with previously certified products.

The certification procedure shall be conducted offline. This allows products to be certified using very large biometric data sets, in repeatable, deterministic and therefore auditable evaluations. Offline evaluation is needed to measure performance when template data is exchanged between all pairs of interoperable products. Large populations shall be used to quantify the effect of sample variance on performance. A template generator is logically a converter of images to templates. A template matcher logically compares one or two templates with one or two templates to produce a similarity score. Template generators and template matchers shall be certified separately. This aspect is instituted because:

1. Template generation is procedurally, algorithmically and physically distinct from matching.

2. Template generation is required by [FIPS], but matching is not.

3. Fingerprint template interoperability is dependent on the quality of the PIV Card templates. The full benefits of an interoperable template will not be realized if a supplier is required to produce both a high performing generator and a high performing matcher.

---

[2] The International Labor Organization's seminal evaluation of interoperable fingerprint templates used "up to three match attempts for each of the primary and secondary finger" for authentication trials. See http://www.ilo.org/public/english/dialogue/sector/papers/maritime/sid-test-report2.pdf

4. Once a template generator is certified and deployed, its templates will be in circulation. It is necessary for all matchers to be able to process these templates. Subsequent certification rounds will be complicated if generators and matchers are certified together.

Separate certification means that a supplier may submit one or more template generators and zero or more matchers for certification. Zero or more of the submitted products shall ultimately be certified.

This test design conforms to the provisions of the currently draft ISO/IEC 19795-4 [ISOSWAP] standard, as profiled by this document. One clause of that standard deals with blind testing: This means that a template matcher shall not be able to discern the source of the enrollment templates.

7.3.1   Template generator

A template generator shall be certified as a software library. For PIV, a template generator is a library function that shall convert an image into a minutiae record. The input image represents a PIV enrollment plain impression. The output template represents a PIV Card template. A supplier's implementation, submitted for certification, shall satisfy the requirements of an application programming interface (API) specification to be published by the test organizer. The API specification will require the template generator to accept image data and produce [MINUSTD] templates conformant to Table 11. Where values or practices are not explicitly stated in Table 11, the specifications of section 3.3.2 and Table 3 apply (e.g. on minutiae type). The CBEFF header and CBEFF signature shall not be included.

The input images shall be provided to the generator using either the Option A or Option B data element specifications given in Table 11. The input data shall be prepared by the test agent.

The test design shall require that template generators produce a conformant template regardless of the input. Such a template may contain zero minutiae. This provision transparently and correctly accounts for failures to enroll. In a deployed system, if quality assessment or image analysis algorithms made some determination that the input was unmatchable a failure to enroll might be declared. In an offline test such a determination shall result in at least a template containing zero minutiae. However because in PIV other suppliers' matchers may be capable of handling even poor templates, it is recommended that a template generator submitted for testing should deprecate any internal quality acceptance mechanism, and attempt production of a viable template.

Table 10: INCITS 381 specification for PIV Card template generator certification

	Required Data Element	PIV Certification Values	Informative Remarks
Option A: Parsed INCITS 381 container, provided as separate parameters to template generator function call			
1.	Finger image data	MIT	Uncompressed pixel data, stored left to right, top to bottom, with one 8-bit byte per pixel. The number of bytes in an image is equal to its height multiplied by its width as measured in pixels.
2.	Finger image quality	20,40,60,80,100	Fingers for which [NFIQ] failed will not be used in certification tests. These values differ from those used in [MINEX].
3.	Finger position	MIT	
4.	Impression type	0	
5.	Vertical line length	MIT	Height
6.	Horizontal line length	MIT	Width
Option B: Un-parsed INCITS 381 container			
1.	Format Identifier (7.1.1)	0x46495200	i.e. ASCII "FIR\0"
2.	Version Number (7.1.2)	0x30313000	i.e. ASCII "010\0"
3.	Record Length (7.1.3)	MIT	
4.	CBEFF Product Identifier (7.1.4)	0	
5.	Capture Device ID (7.1.5)	0	
6.	Image Acquisition Level (7.1.6)	30 or 31	

	Required Data Element	PIV Certification Values	Informative Remarks
7.	Number of Images (7.1.7)	1	
8.	Scale units (7.1.8)	0x02	Pixels per centimeter
9.	Scan resolution (horz) (7.1.9)	197	
10.	Scan resolution (vert) (7.1.10)	197	
11.	Image resolution (horz) (7.1.11)	197	
12.	Image resolution (vert) (7.1.12)	197	
13.	Pixel Depth (7.1.13)	8	
14.	Image compression algorithm (7.1.14)	0	Uncompressed
15.	Reserved (7.1.15)	0	Two bytes, see Note 12 below Table 4
16.	Finger data block length (7.2.1)	MIT	
17.	Finger position (7.2.2)	MIT	
18.	Count of views (7.2.3)	1	
19.	View number (7.2.4)	1	
20.	Finger image quality (7.2.5)	20,40,60,80,100	Fingers for which [NFIQ] failed will not be used in certification tests. These values differ from those used in [MINEX].
21.	Impression type (7.2.6)	0	Live-scan plain impression only
22.	Horizontal line length (7.2.7)	MIT	
23.	Vertical line length (7.2.8)	MIT	
24.	Reserved (FINGSTD, Table 4)	0	One byte, See Note 11 below Table 4
25.	Finger image data (7.2.9)	MIT	Uncompressed pixel data, stored left to right, top to bottom, with one 8-bit byte per pixel. The number of bytes in an image is equal to its height multiplied by its width as measured in pixels.
END OF TABLE			

Table 11: INCITS 378 specification for certification of PIV Card template generators and PIV Card template matchers

	Section title and/or field name (Numbers in parentheses are [MINUSTD] clause numbers)	PIV Conformance Values Allowed	Informative Remarks
1.	Format Identifier (6.4.1)	0x464D5200	i.e. ASCII "FMR\0"
2.	Version Number (6.4.2)	0x20323000	i.e. ASCII " 20\0".
3.	Record Length (6.4.3)	26 ≤ L ≤ 800	26 byte header, max of 128 minutiae. See row 18.
4.	CBEFF Product Identifier Owner (6.4.4)	0	
5.	CBEFF Product Identifier Type (6.4.4)	0	
6.	Capture Equipment Compliance (6.4.5)	0	
7.	Capture Equipment ID (6.4.6)	0	
8.	Size of Scanned Image in x direction (6.4.7)	MIT	Inherited directly from input data
9.	Size of Scanned Image in y direction (6.4.8)	MIT	
10.	X (horizontal) resolution (6.4.9)	197	
11.	Y (vertical) resolution (6.4.10)	197	
12.	Number of Finger Views (6.4.11)	1	
13.	Reserved Byte (6.4.12)	0	
14.	Finger Position (6.5.1.1)	MIT	Inherited directly from input data
15.	View Number (6.5.1.2)	0	
16.	Impression Type (6.5.1.3)	0 or 2	Inherited directly from input data

	Section title and/or field name (Numbers in parentheses are [MINUSTD] clause numbers)	PIV Conformance Values Allowed	Informative Remarks
17.	Finger Quality (6.5.1.4)	MIT	Inherited directly from input data
18.	Number of Minutiae (6.5.1.5)	$0 \leq M \leq 128$	M minutiae data records follow
19.	Minutiae Type (6.5.2.1)	01b, 10b, or 00b	See Note 6 below Table 3
20.	Minutiae Position (6.5.2.2)	MIT	See Note 7 below Table 3
21.	Minutiae Angle (6.5.2.3)	MIT	See Note 8 below Table 3
22.	Minutiae Quality (6.5.2.4)	0	
23.	Extended Data Block Length (6.6.1.1)	0	No bytes shall be included following this field.
END OF TABLE			

Acronym		Meaning
MIT	mandatory at time of instantiation	For PIV Certification, a mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in [FINGSTD]

7.3.2   Template matcher

A template matcher shall be certified as a software library. For PIV, a matcher is a software function that compares enrollment templates with authentication templates to produce a similarity score. The similarity score must be an integer or real value quantity.   The enrollment templates represent the PIV Card templates. The authentication templates represent those extracted from live authentication fingerprints. A supplier's implementation, submitted for certification, shall satisfy the API specification published by the test organizer.

The API specification will support at a minimum the following logical operation: Comparison of one authentication template (from an individual's primary or secondary fingers) with one enrollment template (from either the same or another individual's same finger). Both templates shall conform to the Table 12 profile of [MINUSTD].

The test shall neither prescribe nor prohibit methods whereby fingers' material shall be employed in the core comparison. The only constraint is that all invocations of the matching function shall yield a similarity score regardless of the input templates. Larger scores shall be construed as indicating higher likelihood that the input data originate from the same person. A failure or refusal to compare the inputs shall in all cases result in the reporting of a score. This document recommends implementers report a low score in this case.

The input [MINUSTD] enrollment templates shall be prepared by the test agent using software from a supplier. The input [MINUSTD] authentication templates shall be the output of the template generation software provided by the supplier of the matcher under test.

7.4   Test procedure

The test organization shall publish a test specification document. This document shall establish deadlines for submission of products for certification.

The supplier of a template generator shall submit a request for certification to the test organization. The test organization shall provide a set of samples to these suppliers. This set shall support debugging and shall consist of images conformant to either the A or B specifications of Table 10. The supplier shall submit templates from this data to the test organization. The supplier shall submit the template generator to the test organization. The test organization shall execute it and check that it produces identical templates to those submitted by the supplier.   The test organization shall apply a conformance assessor to the templates. The test organization shall report to the supplier whether identical templates were produced and whether the templates are conformant to the specifications in Table 11.   This validation process may be iterative.

The supplier of a template matcher shall submit a request for certification to the test organization. The test organization shall provide a set of samples to these suppliers. This set shall support debugging and shall consist

of images conformant to either the A or B specifications of Table 10 and templates conformant to the specification of Table 11. The supplier shall submit similarity scores from this data to the test organization. The supplier shall submit the template matcher to the test organization. The test organization shall execute it and check that it produces identical scores to those submitted by the supplier. The test organization shall report to the supplier the result of the check.   This validation process may be iterative.

The test organization shall apply all template generators to the first biometric sample from each member of the test corpus. The test organization shall invoke all template matchers to compare the resulting enrollment templates with second authentication templates from each member of the corpus. The authentication template shall, in all cases, be generated by the matcher supplier's generator. This shall be done for all pair wise combinations of template generators and template matchers. The result is a set of genuine scores for each combination.

The test organization shall invoke all template matchers to compare enrollment templates with second authentication templates from members of a disjoint population. The authentication template shall, in all cases, be generated by the matcher supplier's generator. This shall be done for all pair wise combinations of template generators and template matchers. The result is a set of impostor scores for each combination. The order in which genuine and impostor scores are generated shall be randomized (i.e. it is not implied by the order of the last two paragraphs).

The test organization shall sum the score obtained from matching of images of primary fingers with those obtained from matching of images of secondary fingers. This sum-rule fusion represents two-finger authentication.

7.5   Determination of an interoperable group

The test organization shall compute the detection error tradeoff characteristic (DET) for all pair wise combinations of the template generators and template matchers. The test organization shall generate a rectangular interoperability matrix (see [ISOSWAP]).   The matrix has rows corresponding to the generators and columns corresponding to the matchers. Each element of the interoperability matrix shall be the false reject rate at a fixed false accept rate. This value corresponds to one operating point on the DET. As described in section 7.3.1, the DET automatically includes the effect of failure to enroll and acquire.

An interoperable group of template generators and matchers shall be established as the largest subgroup of products submitted in an initial certification round for which all elements of the interoperability sub-matrix (i.e. FRR values) are less than or equal to 1% at a fixed 1% FAR operating point. The condition that all pair wise product combinations should be below threshold is instituted because the PIV application is intolerant of non-interoperable pairs.

This test procedure identifies products demonstrating core interoperability of minutiae-based technology. This standard does not preclude agencies from conducting subsequent supplementary tests of their own - these might be performance tests of single products or interoperability tests. This standard does not preclude agencies from adopting, for example, more stringent false acceptance rate criteria.

8.   Conformance to this specification

8.1   Conformance

Conformance to this specification will be achieved if an implementation and its associated data records conform to the normative ("shall") sections of sections 3 through 6. The following text summarizes these statements.

8.2   Conformance to PIV registration fingerprint acquisition specifications

Conformance to Section 3.2 requires the use of an [EFTS, Appendix F] certified scanner to collect a full set of fingerprint images and the application of a segmentation algorithm and the [NFIQ]-based quality assurance procedure. Images shall be conformant to this specification if:

1. The acquisition procedures of 3.2 are followed. This may be tested by human observation.

2. The images are conformant to [FINGSTD] as profiled by Table 4 and its normative notes.

3. Testing of images to the requirements of [EFTS, Appendix F].

8.3   Conformance of PIV Card fingerprint template records

Conformance to Section 3.3 is achieved by conformance to all the normative content of the section. This includes production of records conformant to [MINUSTD] as profiled in Section 3.3. Conformance shall be tested by inspection of the records and performing the test assertions of the "PIV Conformance" column of Table 3. Performance certification according to Section 7 is necessary.

8.4   Conformance of PIV registration fingerprints retained by agencies

Conformance to Section 3.4 is achieved by conformance to all the normative content of the section. This includes production of records conformant to [FINGSTD] as profiled in Section 3.4. Conformance shall be tested by inspection of the records and performing the test assertions of the "PIV Conformance" column of Table 4. Quality values [NFIQ] shall be checked against the NIST reference implementation.

8.5   Conformance of PIV background check records

Conformance to Section 3.5 is achieved by conformance to all the normative content of the section. This necessitates conformance to the normative requirements of the FBI for background checks. These shall be tested by inspection of the transactions submitted to the FBI. This inspection may be performed either by capturing the transactions at the submitting agency or at the FBI.

8.6   Conformance to PIV authentication fingerprint acquisition specifications

Conformance to Section 4.2 shall be achieved if certification according to [EFTS, Appendix G] is achieved, and if the resolution and area specifications are met. The Appendix G certification process entails inspection of output images.

8.7   Conformance of PIV facial image records

Conformance to Section 5 shall be achieved by conformance to all the normative content of the section. This includes production of records conformant to [FACESTD] as profiled in Section 5.2. Conformance shall be tested by inspection of records and performing the test assertions of the "PIV Conformance" column of Table 6.

8.8   Conformance of CBEFF wrappers

A PIV implementation will be conformant to section 6 if all biometric data records, whether or not mandated by this document or [FIPS], are encapsulated in conformant CBEFF records. CBEFF records are conformant if:

1. the fields of the Table 8 header are present;

2. the fields of Table 8 contain the allowed values as governed by its normative notes;

3. a digital signature conformant to [800-78] is present;

4. the values are consistent with the enclosed biometric data and the trailing digital signature.

An application that tests conformance of PIV biometric data shall be provided with appropriate keys to decrypt and check the digital signature.

8.9   Conformance of template generators

A template generator shall be certified on the basis of the conformance of its output, its speed of computation, and on the error rates observed when its templates are matched in an interoperability test conformant to Section 7.

A template generator shall be certified if:

1. it converts all input Table 10 [FINGSTD] instances to Table 11 [MINUSTD] templates and these pass the template conformance test suite established by NIST, and

2. it converts 90% of Table 10 [FINGSTD] instances in fewer than 1.3 seconds[3], and

3. all certified matchers verify its output templates with FRR less than or equal to 1% at a FAR of 1%.

8.10 Conformance of template matchers

A template matcher shall be certified on the basis of its speed of computation, and on the error rates observed when it matches templates in an interoperability test conformant to Section 7.

A template matcher shall be certified if:

1. it converts all input Table 11 [MINUSTD] templates to scalar scores, and

2. it executes 90% of the Section 7.4 template matches in fewer than 0.1 seconds, and

3. it matches templates from all certified template generators, and the template generator accompanying the matcher, with FRR less than or equal to 1% at a FAR of 1%.

---

[3] This specification applies to a commercial-off-the-shelf PC procured in 2005 and equipped with a 2GHz processor and 512 MB of main memory. This specification shall be adjusted by the testing organization to reflect significant changes of the computational platform.

9.   Bibliography

Citation	Document
800-73	NIST Special Publication 800-73-1, Interfaces for Personal Identity Verification
800-78	NIST Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification
FIPS	FIPS 201-1 Change Notice 1, Personal Identity Verification, National Institute of Standards and Technology, 2006.
FINGSTD	INCITS 381-2004, American National Standard for Information Technology - Finger Image-Based Data Interchange Format
MINUSTD	INCITS 378-2004, American National Standard for Information Technology - Finger Minutiae Format for Data Interchange
FACESTD	INCITS 385-2004, American National Standard for Information Technology - Face Recognition Format for Data Interchange
CBEFF	INCITS 398-2005, American National Standard for Information Technology - Common Biometric Exchange Formats Framework (CBEFF)
FFSMT	ANSI/NIST-ITL 1-2000 – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, NIST Special Publication 500-245, 2000.
EFTS	IAFIS-DOC-01078-7.1 CJIS-RS-0010 (V7.1) – Electronic Fingerprint Transmission Specification, Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice, May 2, 2005. Linked from here http://www.fbi.gov/hq/cjisd/iafis.htm
	The material at http://www.fbi.gov/hq/cjisd/iafis/efts71/cover.htm may not be fully up to date. Implementers should request the full EFTS documentation, including Appendix N, from the FBI.
SINGFING	See "Personal Identity Verification (PIV): Image Quality Specifications For Single Finger Capture Devices"
	http://www.fbi.gov/hq/cjisd/iafis/piv/pivspec.pdf or http://fips201ep.cio.gov/documents/FBI_PIVspec_071006.pdf
NFACS	IAFIS-DOC-07054-1.0, Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice, April 2004.
MINEX	Minutiae Interoperability Exchange Test. See http://fingerprint.nist.gov/minex04 and the Test Specification: http://fingerprint.nist.gov/minex04/MINEX04API.pdf
NFIQ	NISTIR 7151 - Fingerprint Image Quality, NIST Interagency Report, August 2004
ICS	Methods for Testing and Specification (MTS); Implementation Conformance Statement (ICS) Proforma style guide. EG 201 058 V1.2.3 (1998-04)
ISOSWAP	ISO/IEC 19795:2005 Information Technology — Biometric Performance Testing and Reporting — Part 4: Interoperability Performance Testing